UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,243	12/01/2003	Josh Benaloh	MCS-062-03	1954

7590 05/30/2007

Katrina A. Lyon
LYON & HARR, LLP
Suite 800
300 Esplanade Drive
Oxnard, CA 93036

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,243	BENALOH ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-41 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-7,10-13,16-23 and 26-41 is/are rejected.

7)☒ Claim(s) 8,9,14,15,24 and 25 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see enclosed*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-41 are pending.

Information Disclosure Statement

2. The IDS submitted on 4/26/2004 has been considered. An initialed copy is enclosed.

Claim Objections

3. Claim 16 is objected to because of the following informalities: replace "using the a trusted computing device" with –using a trusted computing device—at lines 10-11. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 11, 17-20 and 30-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 11 recites the limitation "said user's computing device." There is insufficient antecedent basis for this limitation in the claim. For the purpose of this

Office action, it is assumed that the limitation "said user's computing device" is referring to the general purpose computing device as recited earlier in the claim.

7. Claim 19 recites the limitation "the partial signature." There is insufficient antecedent basis for this limitation in the claim. For the purpose of this Office action, it is assumed that Claim 19 is dependent on claim 18 (Claim 18 recites a partial signature).

8. The term "significant" in claims 17-20 and 30-34 is a relative term which renders the claims indefinite. The term "significant" is not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The specification merely cites that the challenge requires the user to expend "significant resources" to answer the challenge; moreover, the specification does not provide any discussion of what constitutes "significant resources" and does not disclose any examples corresponding to the requisite degree that would constitute an expenditure of "significant resources." See Specification, pgs. 22-23.

9. Claims 21 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Claim 22 is dependent on claim 21 and claim 21 is dependent on independent claim 16. Claim 21 recites the limitation "wherein said challenge is generated using information extracted from said user's request for services." However, independent claim 16 only discloses "sending a request for

services including a digitally signed assertion that the challenge has been successfully answered." As a result, claims 21 and 22 recites that the challenge is generated using information extracted from a user's request, wherein the user's request includes a digitally signed assertion that the challenge has been successfully answered. This limitation is not possible as recited.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 35-41 are not limited to tangible embodiments. In view of Applicant's disclosure, specification page 10, lines 14-31, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g. CD-ROM, RAM) and intangible embodiments (e.g. computer readable instructions, data structures per se, signals). As such, the claim is not limited to statutory subject matter.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1-7, 10-13, 16, 17, 23, 35-38 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Hsu et al. USPN 6,038,666 (hereinafter Hsu).

13. As per claim 1, Hsu discloses a computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of: generating a request for services of a service provider at a user's computing device (col. 5:8-14; 7:10-12); generating a challenge at a user's computing device; the user answering the challenge (col. 5:15-18; access requires a fingerprint match); said user's computing device evaluating said user's answer to the challenge (5:18-20) and attaching a digital signature thereto if said user's answer is correct (7:64-8:4); sending said request for services including said digital signature from the user to a service provider (8:4-7); said service provider evaluating said user's request for services and digital signature; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digital signature (8:7-10).

14. As per claim 2, Hsu discloses wherein the user's computing device comprises a trusted computing environment comprising a challenge generator and a secret key. (fig. 3, reference no. 16, 26, 28, 30 and 36; 8:38-41)

15. As per claim 3, Hsu discloses wherein the secret key is used to generate the digital signature. (col. 8:3-4 and lines 38-41)

16. As per claim 4, Hsu discloses wherein symmetric encryption techniques are used to encrypt at least one of said request for services and digital signature. (col. 8:38-41)

17. As per claim 5, Hsu discloses wherein asymmetric encryption techniques are used to encrypt at least one of said request for services and digital signature. (col. 8:3-4 and lines 38-41)

18. As per claim 6, Hsu discloses wherein said digital signature identifies and authenticates the user's trusted device and message data. (col. 8:5-11)

19. As per claim 7, Hsu discloses wherein the message data includes the user's answer to the challenge. (col. 6:24-30, 31-39 and lines 62-63)

20. As per claim 10, Hsu discloses wherein said service provider's determination of whether to allow said user access to said service provider's services is used for one of: assigning an email account; validating an input in a poll; using a search engine; using a chat room; and accessing data on a website. (col. 7:10-13)

21. As per claim 11, Hsu discloses a system for creating a non-interactive human proof, the system comprising: a general purpose computing device; and a computer program comprising program modules executable by the computing device (figs. 2 and

3), wherein the computing device is directed by the program modules of the computer program to, generate a challenge for a computer user using said user's computing device that includes a trusted computing device; require a computer user to answer the challenge (col. 5:15-18; access requires a fingerprint match); send the computer user's answer to the challenge to a service provider with a request to access the computer user's services. (5:8-14; 7:10-12; 8:4-10)

22. As per claim 12, Hsu discloses the system further comprising modules of a computer program to: verify the user's answer to the challenge; and if the user's answer is correct, allow the user access to services provided by the service provider. (8:4-10)

23. As per claim 13, Hsu discloses wherein said trusted computing device comprises a challenge generator and a secret key. (fig. 3, reference no. 16, 26, 28, 30 and 36; 8:38-41)

24. As per claim 16, Hsu discloses a computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of: generating a challenge at a user's computing device for the user using the a trusted computing device resident on the user's computing device; the user answering the challenge (col. 5:15-18; access requires a fingerprint match); sending a request for services including a digitally signed assertion that the challenge has been successfully answered (7:64-8:4); said service provider evaluating said user's request

for services and digitally signed assertion; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digitally signed assertion. (5:8-14; 7:10-12; 8:4-10)

25. As per claim 17, Hsu discloses wherein the process action of generating a challenge comprises generating a challenge that requires that significant resources be expended to answer the challenge. (fig. 3, reference no. 48)

26. As per claim 23, Hsu discloses a computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of: generating a challenge for a user at the user's computing device using a trusted computing device resident on the user's computing device by generating a cryptographic hash of information that is extracted from a message the user generates requesting services from a service provider; the user answering the challenge (col. 5:8-18 [access requires a fingerprint match]; 7:10-12); the user receiving a digitally signed assertion; the user sending a request for services including a digitally signed assertion that the challenge has been successfully answered (7:64-8:7); said service provider evaluating said user's request for services and digitally signed assertion; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digitally signed assertion. (8:7-10)

27. As per claim 35, Hsu discloses a computer-readable medium having computer-executable instructions for determining whether a computer user is human or a computer program, comprising program modules for: generating a request for services of a service provider at a user's computing device (col. 5:8-14; 7:10-12); generating a challenge at a user's computing device; the user answering the challenge (col. 5:15-18; access requires a fingerprint match); said user's computing device evaluating said user's answer to the challenge and attaching a keyed hash thereto if said user's answer is correct (5:18-19; 6:31-39; 7:64-8:4); sending said request for services including said keyed hash from the user to a service provider (8:4-7); said service provider evaluating said user's request for services and keyed hash; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said keyed hash. (8:7-10)

28. As per claim 36, Hsu further discloses wherein the user's computing device comprises a trusted computing environment comprising a challenge generator and a secret key. (fig. 3, reference no. 16, 26, 28, 30 and 36; col. 8:38-41)

29. As per claim 37, Hsu further discloses wherein said keyed hash identifies and authenticates the user's trusted device and message data. (col. 8:5-11)

30. As per claim 38, Hsu further discloses wherein the message data includes the user's answer to the challenge. (col. 8:1-5)

31. As per claim 41, Hsu further discloses wherein said service provider's determination of whether to allow said user access to said service provider's services is used for one of: assigning an email account; validating an input in a poll; using a search engine; using a chat room; and accessing data on a website. (col. 7:10-13)

32. Claims 26 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by McGarvey et al. US Patent Application Number 20030028773 (hereinafter McGarvey).

33. As per claim 26 and 27, McGarvey discloses a computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of: generating a challenge for a user that comprises a partial digital signature using a trusted computing device resident at a trusted third party (figure 1B, reference no. 18; paragraph 36; paragraph 49); the user answering the challenge to complete the digital signature (paragraph 36: "the client signs the nonce with its digital signature"); the user sending a request for services including the complete digital signature (paragraph 36: "and returns the signed nonce to the middle-tier server"); said service provider evaluating said user's request for services and digital signature; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's

request for services and digital signature (paragraph 36: "provides the signed nonce to the back-end servers when access to these servers on behalf of the client is desired"; paragraph 45: "[t]he middle-tier server uses the signed common nonce to access the one or ones of the back-end servers"); wherein the user's computing device computes the portion of the digital signature necessary to complete the partial digital signature (paragraph 36: "the client signs the nonce with its digital signature").

Claim Rejections - 35 USC § 103

34. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

35. Claims 28-30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Billingsley et al. USPN 7,139,916 (hereinafter Billingsley) in view of Remer et al. USPN 6,742,039 (hereinafter Remer) and Stallings Cryptography and Network Security, Chapter 8: Message Authentication and Hash Functions (hereinafter Stallings).

36. As per claim 28, Billingsley discloses a computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of: generating a request for services of a service provider at a user (col. 2:22-26 and lines 30-32); generating a challenge and providing it to said user (2:40-47); the user answering the challenge; the user's answer and request being sent

to the service provider (2:58-63); said service provider evaluating said user's answer and request for services; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of the user's answer. (2:61-67)

37. Billingsley does not disclose using a third party to process the verification of a user when the user requests access to a service provider. However, it is well known in the art at the time of invention for a third party authenticator to function as an arbitrator between two parties. For example, Remer discloses a system and method to connect a device on a protected network using a trusted arbitrator as an intermediary to certify the identity of the user to the protected network. Col. 4:25-42. Remer discloses that such a configuration enables the utilization of a third party arbitrator to reduce overhead processing. Col. 2:28-53. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party to generate the challenge, wherein the trusted third party evaluates the user's answer to the challenge and forwards the request to the service provider if the user's answer is valid. One would be motivated to do so to reduce overhead processing as known in the art. See Remer, ibid.

38. Finally, neither Billingsley nor Remer discloses the third party including a digital signature in the request to the service provider. Stallings discloses using digital signatures as a means to verify that the received message comes from an alleged source, wherein a sender appends a digital signature to a message and a receiver verifies the digital signature. Pg. 238, last paragraph. Such a feature prevents the

manipulation of messages in transit and verifies the source of a message as known to one of ordinary skill in the art. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party to include a digital signature in the request to the service provider, wherein the service provider allows the user access based on the evaluation of the digital signature. One would be motivated to do so to verify that the message is received from the trusted third party. Stallings, ibid. The aforementioned cover the limitations of claim 28.

39. As per claim 29, Billingsley discloses a computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of: a user generating a request for services of a service provider (col. 2:22-26 and lines 30-32); generating a challenge and providing it to said user (2:40-47); the user answering the challenge; the user's answer and request being sent to the service provider (2:58-63); said service provider evaluating said user's answer and request for services; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of the user's answer. (2:61-67)

40. Billingsley does not disclose using a third party to process the verification of a user when the user requests access to a service provider. However, it is well known in the art for a third party authenticator to function as an arbitrator between two parties. For example, Remer discloses a system and method to connect a device on a protected network using a trusted arbitrator as an intermediary to certify the identity of the user to

the protected network. Col. 4:25-42. Remer discloses that such a configuration enables the utilization of a third party arbitrator to reduce overhead processing. Col. 2:28-53. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party to generate the challenge, wherein the trusted third party evaluates the user's answer to the challenge and forwards the request to the service provider if the user's answer is valid. One would be motivated to do so to reduce overhead processing as known in the art. See Remer, ibid.

41. Finally, neither Billingsley nor Remer discloses the third party's submission including a digital signature identifying the third party to the service provider. Stallings discloses using digital signatures as a means to verify that the received message comes from an alleged source, wherein a sender appends a digital signature to a message and a receiver verifies the digital signature. Pg. 238, last paragraph. Such a feature prevents the manipulation of messages in transit and verifies the source of a message as known to one of ordinary skill in the art. As applied to the inventions of Billingsley and Remer, a digital signature appended to the message from the trusted arbitrator to the service provider by the trusted arbitrator identifies the third party as the source of the message. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party's request for services including a digital signature identifying the third party to the service party, wherein the service provider allows the user access based on the evaluation of the digital signature. One would be motivated to do so to verify that the message is received from the trusted third party. Stallings, ibid. The aforementioned cover the limitations of claim 29.

42. As per claims 30 and 33, Billingsley discloses a computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of: a user generating a request for services of a service provider (col. 2:22-26 and lines 30-32); generating a challenge that requires the user to expend significant resources to answer the challenge and providing it to said user (2:40-47); the user answering the challenge; the user's answer and request being sent to the service provider (2:58-63); said service provider evaluating said user's answer and request for services; and said service provider determining whether to allow said user access to said service provider's services based on said evaluation of the user's answer (2:61-67); wherein the challenge is generated using information extracted from the user's request for services. (2:50-53).

43. Billingsley does not disclose using a third party to process the verification of a user when the user requests access to a service provider. However, it is well known in the art for a third party authenticator to function as an arbitrator between two parties. For example, Remer discloses a system and method to connect a device on a protected network using a trusted arbitrator as an intermediary to certify the identity of the user to the protected network. Col. 4:25-42. Remer discloses that such a configuration enables the utilization of a third party arbitrator to reduce overhead processing. Col. 2:28-53. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party to generate the challenge, wherein the trusted third party evaluates the user's answer to the challenge and forwards the request to the

service provider if the user's answer is valid. One would be motivated to do so to reduce overhead processing as known in the art. See Remer, ibid.

44. Finally, neither Billingsley nor Remer discloses the third party's submission including a digitally signed assertion that the challenge has been successfully answered to a service provider. Stallings discloses using digital signatures as a means to verify that the received message comes from an alleged source, wherein a sender appends a digital signature to a message and a receiver verifies the digital signature. Pg. 238, last paragraph. Such a feature prevents the manipulation of messages in transit and verifies the source of a message as known to one of ordinary skill in the art. As applied to the inventions of Billingsley and Remer, a digital signature appended to the message from the trusted arbitrator to the service provider is a digitally signed assertion that the user is certified. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the third party's request for services including a digitally signed assertion that the challenge has been successfully answered to a service provider, wherein the service provider allows the user access based on the evaluation of the digital signature. One would be motivated to do so to verify that the message is received from the trusted third party. Stallings, ibid. The aforementioned cover the limitations of claims 30 and 33.

Allowable Subject Matter

45. Claims 8, 9, 14, 15, 24 and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See enclosed PTO-892.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung Kim
May 22, 2007